

CLAIMS:

1. A system for communicating data and protecting rights therein, comprising:
at least one user device for receiving data;
a server in communication with said at least one user device and including a trusted lock;
a rights management engine for determining user rights in said data;
a storage device for storing said data; and
a storage device for recording an audit trail.

2. A system according to claim 1, wherein said server, rights management engine, data storage and audit trail storage are in a secure location separate from the user device so that trusted services including trusted timing, auditing and copying are performed in a secure environment.

3. The system according to claim 1, wherein said user device includes a storage device for holding data which is released under instructions from said server.

4. The system according to claim 1, wherein said server and user device are connected through a wireless connection.

5. The system according to claim 4, wherein said wireless connection is an "always on" connection.

6. A method of communicating data from a server to a user device and protecting rights therein, comprising:
authenticating identification of said server and said user device;
requesting data to be communicated;

5 authorizing said data to be communicated based on rights attributed to said user device;
6 recording said authorization to provide for billing information and an audit trail;
7 communicating said data to said user device.

1 7. The method according to claim 6, wherein said data is communicated to said user
2 device and stored therein and rendered in sections according to instructions communicated from
3 said server.

1 8. The method according to claim 6, wherein communication between said server and said
2 user device is a wireless communication.

1 9. The method according to claim 8, wherein said wireless communication is an "always
2 on" connection.

1 10. The method according to claim 6, wherein said authorization step is performed by a
2 digital rights management engine in communication with said server.

1 11. The method according to claim 6, wherein said recording step is performed in a
2 storage device to record authorization along with time and other information in order to provide a
3 trusted audit trail, which is based on trusted time and a trusted third party to sign the recording.

1 12. The method according to claim 6, wherein said data is originally stored in a content
2 storage device connected to said server.

1 13. A rights secure communication device for providing data to a user device comprising:

2 a server;
3 a data storage device connected to said server for storing said data; and
4 a digital rights management engine connected to said server for determining rights
5 attributed to users.

1 14. The communication device according to claim 13, further comprising a secure storage
2 device for recording authorization of data communication in a secure audit trail.

1 15. The communication device according to claim 13, wherein data is sent from said
2 server to a user through a wireless communication system.

1 16. The communication device according to claim 15, wherein said wireless
2 communication system is a “always on” connection.

1 17. A mobile terminal system for receiving protected data, comprising:
2 a wireless connection including a transmitter and receiver for communicating with a server
3 which stores protected data, stores data relating to rights to use said protected data and the
4 storage device for recording transactions relating to said protected data;
5 a decryption engine for decrypting encrypted data sent from said server through said
6 wireless connection;
7 a display device for displaying said protected data to a user of said mobile terminal.

1 18. The method according to claim 17, wherein said mobile terminal includes a data
2 storage device for temporarily storing protected data.

